Federal PKI
Management Authority
Enabling Trust

Path Discovery and Validation (PD-VAL) Product Conformance

TECHNICAL TEST REPORT

[Ascertia ADSS SCVP Server]

VERSION 1.1.0

June 14, 2012

FINAL

SENSITIVE BUT UNCLASSIFIED

PREPARED BY PROTIVITI GOVERNMENT SERVICES
FOR GENERAL SERVICES ADMINISTRATION

TABLE OF CONTENTS

TABLES

1 Scope and Specifications

The Federal Public Key Infrastructure Management Authority (FPKIMA) tested Ascertia's Advanced Digital Signature Services (ADSS) Server-based Certificate Validation Protocol (SCVP) Server against the two National Institute of Standards and Technology (NIST) Public Key Infrastructure (PKI) test suites

1) Public Key Interoperability Test Suite (PKITS) for Certification Path Validation; Version 1.0.1; April 14, 2011
    a) NIST Recommendation for X.509 Path Validation
2) Path Discovery Test Suite; Version 0.1.1; June 3, 2005

The ADSS SCVP Server utilizes the 1.3.6.1.5.5.7.17.1 Object Identifier (OID) and the 1.3.6.1.5.5.7.17.3 OID, to represent the [id-stc-build-status-checked-pkc-path] certChecks and the [id-stc-build-pkc-path] certChecks, respectively, as defined in RFC 5055. Ascertia declares that ADSS SCVP Server supports Delegated Path Discovery (DPD) and Delegated Path Validation (DPV) when using these certChecks, respectively. ADSS SCVP Server does not currently support the [id-stc-build-valid-pkc-path] certChecks.

The FPKIMA did not attempt to use this testing to validate the proper use of these certChecks or the associated OIDs.

1.1 Technical Specifications

Specifications of the ADSS SCVP Server used to execute the tests are as follows:

a) Relevant software version: ADSS SCVP Server Patch Version 4.5.1.4, Build 4514.4510.280312.9150
    (1) ADSS SCVP Server 4.5.1.4 was provided by Ascertia on 3/29/2012
b) ADSS Server was implemented on an FPKIMA Test Server:
    (1) CPU: Dual Intel(R) Xeon(R) E7310 @ 1.60GHz
    (2) RAM: 4.06 GB
    (3) Operating System: 64 Bit Windows Server 2008 R2 Enterprise, Service Pack 1

Specifications of client used to execute the tests:

a) ADSS Server Test Tool Version 4.5.1, provided by Ascertia on 9/6/2011
b) ADSS Test Tool was implemented and run from a computer with the following specs:
    (1) CPU: Intel(R) Core(TM) M520 @ 2.40GHzBE
    (2) RAM: 4.00 GB
    (3) Operating System: 64 Bit Windows 7 Enterprise

2 Path Validation Testing Program Report

In NIST Recommendation for X.509 Path Validation, some tests are identified as applicable to all applications, some are identified as applicable to applications that support particular services, and some are identified as not necessary to run. The tests that are not necessary to run are intended to be useful in evaluating particular application features that may or may not be supported. Competent applications that are compliant with all relevant standards may not necessarily pass these tests. These tests were included in this testing process, and are referred to as the "non-required" tests.

Tests were executed using the ADSS SCVP Server DPV functionality:

a) DPV requests are identified to the ADSS SCVP Server from the ADSS Server Test Tool by use of the 1.3.6.1.5.5.7.17.3 (id-stc-build-status-checked-pkc-path) OID, as the "certChecks" argument in the command

The following subsections summarize the tests that were executed:

a) Section 2.1 describes testing using the NIST test repositories for dynamic data lookup; and
b) Section 2.2 describes testing with all of the CA certificates and CRLs imported into the ADSS Server Trust Manager.

2.1 Dynamic Testing Using the NIST TEST Repositories

a) A single trust anchor certificate is provided with the test suite for all 247 tests. The "Trust Anchor" CA certificate was the only certificate installed in the ADSS Server Trust Manager. ADSS SCVP Server was able to retrieve relevant Certificate Revocation Lists (CRLs) and other certificates to build the appropriate paths to the trust anchor certificate, from the specified locations in the NIST repositories. ("specified locations in the NIST repositories" are detailed within the certificate references, starting with the end entity certificate presented for each test case)
b) Results using this configuration:
    - Total number of tests = 247
    - Number of tests that return the appropriate expected validation response ("Success" or "Failed"), as indicated in the Test Suite document = 246
    - Total number of issues identified = 1
    - (Issues involving non-required tests = 1)
    - Total number of applicable issues = 0
    - Table 1 details the PKITS Path Validation Test Issues

TABLE 1 PKITS PATH VALIDATION TEST ISSUES – DYNAMIC DATA RETRIEVAL

PKITS PATH VALIDATION TEST ISSUES – DYNAMIC DATA RETRIEVAL	
TEST # & DESCRIPTION	EXPLANATION
TEST APPLICABILITY	
EXPECTED RESULT	
4.3.8 Valid RFC3280 Optional Attribute Types	Does NOT conclusively pass this test (when using the NIST repositories for dynamic data retrieval): 4.3.8 returns a "Failed" response when using external NIST repositories for data retrieval, but returns a "Success" response when using imported test data. One or more of the various optional attribute types used in the subject name field may not be supported.
This test does not need to be run	
Successful Validation	

2.2 Testing with all CA Certificates and CRLs Stored in ADSS SCVP Server

a) All CA certificates and CRLs were installed (or attempted to be installed) in the ADSS Server Trust Manager, so certificate path building and validation could be performed at the ADSS SCVP Server with no need to follow the certificate references to external locations.

b) Some tests did not allow the import of the associated CRLs, for the same reasons that the test is expected to produce an invalid response. These tests then produce an invalid response because there is no CRL available for validation. This is considered an acceptable response.

c) Results using this configuration:
   - Total number of tests = 247
   - Number of tests that return the appropriate expected validation response (“Success” or “Failed”), as indicated in the Test Suite document = 246
   - Total number of applicable issues = 1
   - Table 2 details the PKITS Path Validation Test Issues

TABLE 2 PKITS PATH VALIDATION TEST ISSUES – STATIC DATA

PKITS PATH VALIDATION TEST ISSUES – STATIC DATA	
TEST # & DESCRIPTION TEST APPLICABILITY EXPECTED RESULT	EXPLANATION
4.1.5 Valid DSA Parameter Inheritance Run only if application can verify DSA signatures and parameter inheritance Successful Validation	Does NOT conclusively pass this test (with certificate path and CRL data stored at the server): 4.1.5 returns a "Success" response when using external NIST directory for data retrieval. When attempting to use imported test data, the CRL import fails for the CRL associated with the "DSA Parameters Inherited CA," and the test returns a "Failed" response (CRL import is required when using imported CA certificates).

2.3 Miscellaneous Comments

Nine tests (4.8.15, 4.8.16, 4.8.17, 4.8.18-1, 4.8.18-2, 4.10.12-1, 4.10.12-2, 4.10.13, and 4.10.14) involve User Notice Qualifiers in the Certificate Policies extension of certificates, with specific user notices expected to be displayed depending on the certificate policy processing. Each of these tests is identified in NIST Recommendation for X.509 Path Validation as a non-required test (or the test is required, while the user notice portion of the test is identified as "irrelevant").

Although ADSS SCVP Server does not display the user notices and does not appear to support this feature, all nine of these tests returned the appropriate expected validation response ("Success") and the FPKIMA considers these tests as passed.

3 Path Discovery Testing Program Report

The path discovery tests were executed using the NIST test repositories for dynamic data lookup:

a) Three test trust anchor CA certificates are provided with the test suite (Basic Directory Trust Anchor, Basic HTTP URI Trust Anchor, and Basic LDAP URI Trust Anchor), which were installed in the ADSS Server Trust Manager. ADSS SCVP Server was able to retrieve relevant Certificate Revocation Lists (CRLs) and other certificates to build the appropriate paths to these trust anchor certificates, from the specified locations in the NIST repositories. ("specified locations in the NIST repositories" are detailed within the certificates, starting with the end entity certificate presented for each test case).

The following subsections summarize the tests that were executed:

a) Section 3.1 describes testing with ADSS SCVP Server DPD functionality; and
b) Section 3.2 describes testing with ADSS SCVP Server DPV functionality.

3.1 Testing with DPD Functionality

(1) DPD requests are identified to the ADSS SCVP Server from the ADSS Server Test Tool by use of the 1.3.6.1.5.5.7.17.1 (id-stc-build-pkc-path) OID, as the "certChecks" argument in the test commands
(2) The ADSS SCVP Server Transaction Log Viewer demonstrates that the appropriate certificate path and supporting CRLs are being discovered for all 39 test cases
(3) The test commands were run with "revocation_info, all_cert_paths" as a "wantBacks" argument, so copies of all certificates and CRLs necessary to build the path are retrieved and stored as files at the operating system
    (a) Copies of all necessary certificates and CRLs are retrieved for all 39 test cases
(4) ADSS SCVP Server returns a "Success" response for all test cases, including those that involve a revoked certificate. No validation is being performed.
(5) The DPD functionality has not been tested in conjunction with a client validation application.

3.2 Testing with DPV Functionality

(1) DPV requests are identified to the ADSS SCVP Server from the ADSS Server Test Tool by use of the 1.3.6.1.5.5.7.17.3 (id-stc-build-status-checked-pkc-path) OID, as the "certChecks" argument in the command

(2) Results using this configuration:

- Total number of tests = 39
- Number of tests that return the appropriate expected validation response ("Success" or "Failed"), as indicated in the Test Suite document = 38
- Total number of applicable issues = 1
- Table 3 details the Path Discovery Test Issues

TABLE 3 PATH DISCOVERY TEST ISSUES – ADSS DPV SERVICE

PATH DISCOVERY TEST ISSUES – ADSS DPV SERVICE	
TEST # & DESCRIPTION **TEST APPLICABILITY** **EXPECTED RESULT**	**EXPLANATION**
4.2.3.1 Basic Combined Mesh Path Discovery Discovery of a non-hierarchical mesh path of certificates with HTTP URIs, LDAP URIs, and no URIs Successful Validation	Does NOT conclusively pass this test: Test 4.2.3.1 was attempted several times, and let run for several hours (overnight on one occasion). A response has never been received in the ADSS Server Test Tool command window. After one (and only one) of the attempts, while testing with ADSS SCVP Server 4.5.1.3, a response was recorded in the ADSS SCVP Server Transaction Log Viewer even though the test attempt had been stopped several hours earlier than the response was recorded. The log record indicates: ▪ The test response was "Failed" with an error code "Certificate is not trusted" (the appropriate expected result is "Success") ▪ The Request Time was 13:29 and the Response Time was 3:43 on the following day (14 hour lag time). ▪ During the validation of the CA certificate [cn=CA, ou=Basic Combined OU4, o=Test Certificates, c=US] ADSS appears to be unable to validate the CRL issuer CA certificate [ou=Basic Directory Bridge CA, o=Test Certificates, c=US] ❖ Even though the same log record appears to indicate that this same CA certificate [ou=Basic Directory Bridge CA, o=Test Certificates, c=US] was successfully validated earlier in the path validation process.

3.3 Miscellaneous Comments

When using "revocation_info, all_cert_paths" as a "wantBacks" argument in the test commands, copies of all certificates and CRLs necessary to build the path are retrieved and stored as files at the operating system. For six test cases (4.1.1.5, 4.1.1.6, 4.1.2.9, 4.1.2.10, 4.1.2.13, and 4.1.2.14): two copies (i.e., a redundant copy) of the intermediate CA certificate used to certify the CRL that validates the end entity certificate are retrieved and stored as files at the operating system, and two copies (i.e., a redundant copy) of the CRL that validates the end entity certificate are retrieved and stored as files at the operating system. It is an unnecessary use of resources to retrieve and store redundant copies of these certificates and CRLs, and this condition only occurs with the six test cases identified above, but the FPKIMA does not consider that a failing condition.